Brainwave: A Multidisciplinary Journal (ISSN: 2582-659X), Vol. 3, Special Issue , March 2022, pp. 35-42, © Brainware University

A Comparison Study on Trust-Based Routing Protocols In MANET

Joydeep Kundu
Brainware University, Kolkata
joydeepkundu.1988@gmail.com

Abstract – Nodes (dynamic hubs) moves through wireless links without any fixed infrastructure in MANET. These properties make it vulnerable to any kind of new security attacks which absent in a traditional wired network. The routing protocols play an important role in transferring data. Mainly two basic routing such as cryptographic and trust based mechanism are used in ad-hoc network. Cryptographic mechanisms are used in routing protocols to secure data packets while transmitted in the network. The fundamental goal of cryptography is to address the confidentiality, data integrity, authentication, and non-repudiation in information security. But cryptographic techniques incur a high computational cost and can't identify the nodes with malicious intention. So, employing cryptographic techniques in MANET are quite impractical as MANETs have limited resource and vulnerable to several security attacks. Therefore trust mechanism is used as an alternative to the cryptographic technique. There are several trust based protocols have been proposed for MANET. So in this paper comparison analysis of several trust based protocol has been done based on the advantages and disadvantages.

Keywords-- MANET, Trust, Cluster based, AMLeT, CONFIDANT, CORE, Elapsed time.

Introduction

MANET [1-2] stands for mobile ad-hoc network, where mobile signifies randomly changing, Ad-hoc for infrastructure less network & network that connect all mobile nodes to form a temporary network. So when a collection of mobile nodes form a temporary network without any well-defined infrastructure, then the wireless network is known as a mobile ad- hoc network (MANET). MANETs are distributed in nature, and also perform at any place without any access points. This property of MANET makes itself flexible and robust. Therefore it is broadly used in military battlefield, emergency purposes for disaster relief (such as in fire, flood) and even class room, conference hall also. All the distributed nodes in MANET act like a router. Each node has wireless transmitter and receiver with it, so that it can communicate with each other in a wireless environment. In this network nodes are responsible to establish and maintain the routes for successful transmission of packets or messages to the destination. Nodes which are far away from the network can also participate with the help of intermediate nodes.
This paper contains four sections. At first, we discuss about different types of an existing trust model with their unique features. Section 2 presents a comparison table which is based on advantages and drawbacks of the above mentioned trust model. Comparison table & Comparison analysis is explained briefly in section 3 & r respectively and conclusion is described in section 4.

Related Work

MANET routing protocols are essential to detect nodes with malicious intention and avoid them during the selection of trusted route to improve the performance of the network. In this section we discuss about various types of trust based routing schemes with their unique mechanism.

Cooperation of Nodes: Fairness in Dynamic Ad-Hoc Networks (CONFIDANT)

CONFIDANT protocol was established in the year 2002 by [3]. This model extracts those nodes from the network which behave as non co-operative (misbehaving). Basic principle of this protocol is, at first a node selects a path based on the trust relationship of other intermediate nodes. Trust relationship is established by the past experience of routing & forwarding behavior of intermediate neighbor nodes. Every node observes (monitors) the behavior of other intermediate nodes. Then alarm messages are sent to all intermediate nodes whenever non-cooperative node is detected. Whenever a non-cooperative node is found then all other nodes avoid that node at the time of selecting the route in MANET [4-6]. There are four components of CONFIDANT, such as monitor, trust manager, reputation system & path manager.

CORE: (A collaborative reputation mechanism to encode node co operation in Mobile ad-hoc network (MANET)

CORE model was proposed by [7] in 2002.This model works on cooperative behavior of the mobile nodes. Its basic principle is to differentiate between misbehaving and cooperative nodes. It uses reputation table and watchdog mechanism for identifying such nodes. CORE further differentiates the misbehaving nodes into selfish and malicious nodes. The selfish node which not cooperates with neighbors and saving power (battery) for their communications but do not destroy its neighbors. A malicious node in MANET [8] not only behaves abnormally but also destroys its neighbor. The components of reputation table maintain the intermediate node's table associated with their ratings. Reputation value is provided by watchdog component after calculating the function. There are three types of reputations exist in CORE model: Subjective Reputation, Indirect Reputation, and Functional Reputation.

LARS (Locally Aware Reputation System):

LARS (Locally Aware Reputation System) trust schema was established in the year 2006 by [9]. This model is used to identify the selfish behavior of a node. Basically, LARS calculates the performance of a node with its reputation value. It gives reputation value to its all one hop neighbors in the network. This reputation value of neighbor nodes may be modified by the direct observation of a node. In this model, every node can produce alert message to its neighbors, when its trust value falls beyond the threshold value. Here, two types of misbehavior of a node such as packet dropping and false reputation rating are considered. In LARS, node's reputation is evaluated from direct observation only. The exchange of second hand information is not allowed in this protocol. The value of node's reputation will be reducing if it discards the packets. Note that in LARS model, global reputation value is not calculated, and also no reputation message is distributed over the network. The trust reputation value TR changes in the range $[TR_{min}, TR_{max}]$.There are two threshold, TR_g for good reputation and TR_b for bad reputation, where the relationship among the reputation are as follows: $TR_{max} > TR_g > TR_b > TR_{min}$. LARS provides three possible behavior of a node N with reputation value TR from the above relation,

1. N is not selfish, if $TR_g < TR < TR_{max}$,
2. N is selfish, if $TR_{min} < TR < TR_b$,
3. Cannot decide whether N is selfish or not, if $R_g < R < R_b$.

A new node will be given a reputation value within the range$[TR_g, TR_b]$, when it either entered into the network or joined to a new neighborhood because new node cannot be identified by the members of the new neighborhood whether it is non-cooperative or not.

Cluster based trust routing model

Cluster based trust model was introduced by [10-17] in 2008.The technique of dividing the network into interconnected substructures is called clustering and the interconnected substructures are called clusters. A cluster consists of three types of nodes - ordinary nodes, gateway nodes and cluster heads. Ordinary nodes are cluster members but they do not have neighbors belonging to different clusters. Gateway nodes are nodes in a non-cluster head state located at the boundary of a cluster. They are used for routing to a node from a different cluster. Networks select a set of nodes that can serve as the backbone of the network. A network can contain a number of clusters and each cluster has cluster head and cluster members, which are at one hop away from the cluster head. The cluster head of one cluster is connected to another cluster directly or through the gateway nodes. The gateway nodes and the cluster heads together manage the routing mechanism of the network. The cluster head allocates the resources to the other nodes in the network. It must perform extra work with respect to other nodes in the network. There are two types of routing in the cluster-based model, i.e. inter-routing & intra-routing. Routing within the cluster is known as intra-routing & routing among the cluster is inter-routing [18-20].

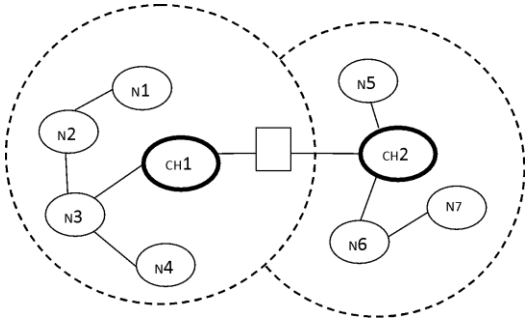

Fig I: Clustering Model

Calculation of node trust:

The trust value of one node (let j) on another node (let k) depends on the correct forwarding of packets by node k. Here, TR_{jk} represents the direct trust on k by node j. Now the value of TR_{jk} at time t is shown by the following equation:

$$TR_{jk}(t) = w1 * CFR_{jk}(t) + w2 * DFR_{jk}(t) \qquad (1)$$

Where CFR_{jk} (t) is control packet forwarded ratio & DFR_{jk}(t) is the data packet forwarded ratio observed by node j at time t for forwarding node k.w1, w2 are the weights assigned to CFR and DFR. Node j checks whether node k correctly sent the data packet or not, after each transaction. So if neighbor node k of the node j successfully forwards the data packets, then the trust value of TR_{jk} will increase otherwise not. The following table has shown the multiple level of trust on a node based on trust value. The range of trust value from 0 to 1.Here, 0 means no trust and 1 stand for complete trust. The trust values in between 0 and 1 signify various trust levels, which have shown in table below. The trust value more than 0.5 means success probability is more than failure and less 0.5 means failure probability is more than success probability.

LEVEL	TRUST VALUE	MEANING
1	[0,0.5]	Malicious
2	[0.5,0.85]	Suspicious
3	[0.85,0.95]	Less trustworthy
4	[0.95,1]	Absolute Trustworthy

Table I. Trust Level of nodes

Computation of route trust:

When the source node establishes a route to a destination by the forwarding message among the intermediate nodes, then the value of route trust is computed through the trust values of nodes among the routes.

Node ID
N_C and N_A control packets
N_C and N_A data packets
Packet buffer

Table II. Framework of trust record list

TR_p (t_i) is the route trust of the route p, that is calculated by the following formula.

$$TR_p(t_i) = min(\{N_j, N_k \in P \text{ and } N_j \rightarrow N_k\}) \quad (2)$$

Where N_j, N_k are any two adjacent nodes among the route P. $N_j \rightarrow N_k$ means N_j forwards packet to the N_k through the route P and N_k is the next hop node of node N_j.

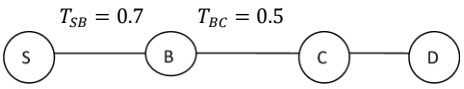

Fig II. Single route trust

Node trust of node S on B is expressed by a direct edge T_{SB} whose value is 0.7. The path trust value between sources to destination is the product of all intermediate node trust values. Therefore $T_{p(S,B,C,D)} = T_{SB}.T_{BC} = 0.7 * 0.5 = 0.35$.

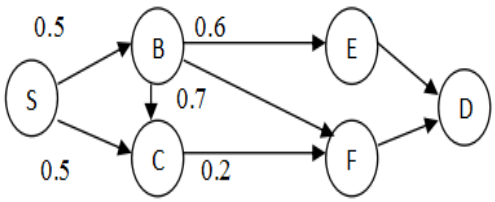

Fig III: Multiple route trusts

The path $T_{p(S,B,C,F,D)} = 0.07$ is the most trustworthy route among four possible paths in the given complex graph as shown in Fig III. Therefore, Path trust denotes a joint probability at which packets will be forwarded if they are sent along the path.

Route Strategy:

In route strategy phase, when a source node wants to send a data, it tries to look up the destination in its routing table. If there is a destination node in that routing table or a node that has the route to the destination, source node then selects that route and sends data to the destination.

Adaptive Multi Level Trust framework for MANET (AMLeT):

Adaptive multi level trust framework (AMLeT) [21] was established in the year 2011. Mainly, there are two levels of trust in AMLeT such as hard and soft trust. At first, this model measures the trust value either by using hard or soft level of trust. Then update the computed trust values by considering various scenarios of the network layer with respect to time. Finally, AMLeT based AODV routing schema has been established by improving overall network performance. This trust framework does not depend on particular overhead time in the network functions.

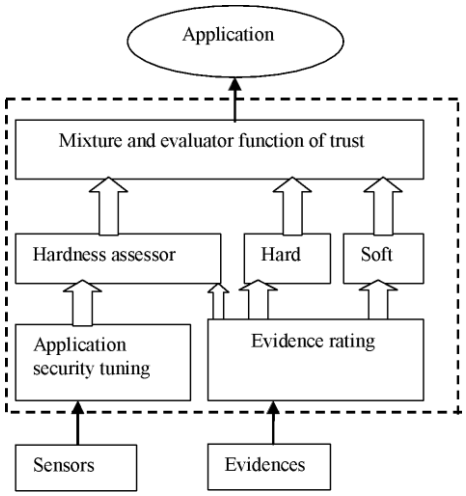

Fig IV. AMLeT trust framework

Comparison Table Of Discussed Trust Models:

Existing Protocol	Advantages	Disadvantages
1. Cooperation of Nodes: Fairness in Dynamic Ad-Hoc Networks (CONFIDANT) (2002).	1. CONFIDENT protocol can efficiently identify and delete the non-cooperative nodes from the ad-hoc network. 2. It can identify the non cooperative nodes by sending alarm message to its all intermediate nodes.	1. Initially this model assumes that all participated nodes into the network are authenticated. 2. It also assumes that nodes do not betray as non-cooperative with their neighbors in the network.

2. CORE: (A collaborative reputation mechanism to encode node co operation in Mobile ad-hoc network) (2002).	1. It prevents the denial of service attacks. 2. It can differentiate selfish nodes from malicious node in the ad-hoc network.	1. CORE does not provide the concept about second-chance authentication mechanism in MANET.
3. LARS (Locally Aware Reputation System)(2006)	1. LARS mechanism is simple and distributed. 2. It can detect two types of selfish behavior of a node, such that extreme selfishness and selective selfishness.	1. LARS cannot do better in higher mobility scenarios. Higher mobility scenario means where neighborhood nodes change randomly and reputation table will also refresh rapidly. 2. This model does not focus its performance scenario with threshold, detection time and false positive rate.
4. Cluster-Based Trust routing model (2008).	1. This model calculates the dynamic trust values of nodes and also increases the efficiency of MANET. 2. Previous information is not required for calculating the trust value of nodes in MANET.	1. Performance will be decrease by increasing the size of cluster in MANET. 2. It is applicable only for the small size ad-hoc network.
5. Trust-based On-demand Multipath Routing in Mobile Ad Hoc Networks (TAODV) (2009).	1. Trust based AODV can detect malicious node and selfish node in MANET. 2. TAODV has achieved remarkable performance in packet forwarding ratio and detection of malicious attacks in ad hoc network.	1. There is no concept about authentication mechanism of nodes.
6. AMLeT: Adaptive Multi Level Trust framework for MANETs (2011).	1. The trust framework of AMLeT is flexible and also efficiently used in various scenarios of network application. 2. Network performance of this model does not depend on particular overhead time in network operations.	1. It is inefficient to operate as more adaptive in various scenarios of network at the time of high security requirement.

Comparison Analysis

Resource constrains such as limited bandwidth, power (battery), and computational power are the main drawbacks of an MANET [22-23]. It also lacks of reliable centralized administration. MANETs are easily

affected by various types of attacks such as wormhole attack, fabrication attack, impersonation attack, Denial of Service attack, etc. due to its infra-structure less network. Therefore various types of trust based routing mechanisms are proposed to prevent such types of attacks. CONFIDANT protocol, can efficiently detect non-cooperative nodes by sending alarm message, to its all intermediate nodes, and path manager component deletes that non-cooperative nodes from the selected path (route). But if the attacker (malicious node) sends false alarm messages then good nodes also taken as non cooperative nodes and at last they are deleted by the path manager. Obviously, network performance drops rapidly. The above attack is known as **fabrication attack**, which basically generates a false (wrong) message to its neighbor into the ad-hoc network. In CONFIDANT protocol, node's reputation increase when it sends the packets to its neighbor. So the malicious node will increase its reputation value by creating a tunnel within the network. This type of attack is called **wormhole attack**. Reputation schemas such as CORE, LARS, OCEAN, CONFIDANT has been proposed for detecting the selfish behavior of a node in MANET. CONFIDANTS, CORE, LARS use direct reputation of a node. That means, AMLeT adapts itself according to context and situations changes of network. Feasibility and functionality of the model has proved by AMLeT based AODV routing protocol. The evaluated trust values (numeric) by this model shows that the modified AODV routing protocol increases the network efficiency with respect to overhead time.

Conclusion And Future Work

In this paper, we survey some existing trust based routing models, which achieve trustworthiness among distributed nodes in MANET. It has observed that, protocol based trust models like CONFIDANT, CORE measured the trust values by the direct communication whereas system based trust models like TAODV calculates the same with the help of indirect interaction between the nodes in MANET. System based trust model also use the concept of punishment and reward for malicious and co-operative nodes in MANET respectively. On the other hand, Cluster based trust model measures the trust value directly (within one cluster) and indirectly (among multiple clusters) in ad-hoc network. All the above-mentioned routing protocols are improved with new concept and strategies to achieve trustworthiness and reliability in MANET routing and extracting the non-cooperative nodes which reduce the network performance. AMLeT based trust model improves the network performance by increasing the quality of service (QoS) metrics into the network.

After going through the various trust based existing approaches, we have seen that some protocol only focus on the improvement over the performance through trust mechanisms without focusing on the security attacked by malicious nodes within the network and some protocols focus only on security not on the performance. In future, we plan to implement a trust model which improves the performance of the network.

References

[1] Renu Dalal, Manju Khari and Yudhvir Singh.(2012). Different Ways to Achieve Trust in MANET. *International Journal on AdHoc Networking Systems (IJANS), 2(* 2).

[2] Goyal, Priyanka, Parmar, Vinti, and Rishi, Rahul (2011). MANET:Vulnerabilities, Challengs, Attacks,Application. *IJCEM International Journal of Computational Engineering & Management,11*.

[3] Buchegger, Sonja & Le Boudec, Jean-Yves. (2002). Performance analysis of the CONFIDANT protocol. 226-236. 10.1145/513800.513828.

[4].X. Liu and X. Zhang. (2020). NOMA-Based Resource Allocation for Cluster-Based Cognitive Industrial Internet of Things. *IEEE Transactions on Industrial Informatics,16*(8), 5379-5388. DOI: 10.1109/TII.2019.2947435.

[5]. X. Liu, X. Zhai, W. Lu, and C. Wu. (2021) . QoS-guarantee resource allocation for multi-beam satellite industrial internet of things with NOMA. *IEEE Transactions on Industrial Informatics, 17(*3), 2052–2061.

[6]. S. J. Wen and C. H. Huang. (2018). Delay-aware cross-layer optimization method for FANET. *Journal on Communications, 39*(4),1–12.
[7] Michiardi P., Molva R. (2002). Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks. In: Jerman-Blažič B., Klobučar T. (eds) *Advanced Communications and Multimedia Security. IFIP — The International Federation for Information Processing*. Boston: Springer,
[8] Marti, S., Giuli, T. J, Lai,k., Baker, M.(2000). Mitigating Routing Misbehavior in Mobile Ad-hoc Networks. *ACM MobiCom conference,*
[9] Jiangyi Hu and Mike Burmester (2006). LARS - A Locally Aware Reputation System for Mobile Ad Hoc Networks. *ACM SE'06* .
[10] CHEN Aiguo, XU Guoai and YANG Yixian ," A Cluster-Based Trust Model for Mobile Ad hoc Networks"
[11] Rajib K.Nokkanti and Chung-wei Lee,"Trust Based Adaptive On demand Ad Hoc Routing Protocol",ACMSE'04,April23,2004,Huntsville,USA.
[12] Li, Xin, Jia, Zhiping, Wang and Haiyang, "Trust-based On-demand Multipath Routing in Mobile Ad Hoc Networks", School of Computer Science and Technology, Shandong University, High-tech Development-Zone, Ji'nan 250101, Shandong Province, People's Republic of China, www.ietdl.org.

[13] M. Karthigha; L. Latha; K. Sripriyan, A Comprehensive Survey of Routing Attacks in Wireless Mobile Ad hoc Networks, 10.1109/ICICT48043.2020.9112588, 19687142.

[14] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao and Chin-Feng Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", *IEEE Systems Journal*, vol. 9, no. 1, 2015.

[15] S. Gurung and S. Chauhan, "A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET", *Wirel. Netw*, pp. 1-11, 2019.
[16] S SankaraNarayanan and G Murugaboopathi, "ModifiedsecureAODVprotoco ltopreventwormholeattackinMANET", *ConcurrencyComputatPractExper*, 2018.
[17] J. S. Raj, "Qos optimization of energy efficient routing in iot wireless sensor networks", *Journal of ISMAC*, vol. 1, no. 01, pp. 12-23, 2019.
[18] A. Dinesh Kumar and S. Smys, "An energy efficient and secure data forwarding scheme for wireless body sensor network", *International Journal of Networking and Virtual Organisations*, vol. 21, no. 2, pp. 163-186, 2019.
[19] S B Mohan Kumar, K M Anand Vijay and N S Suhas, "A Policy based preventive measure against flooding attack in MANETs", *IEEE International Conference On Recent Trends In Electronics Information Communication Technology*, 2016.
[20] M Sathish, K Arumugam, S. NeelavathyPari and V S Harikrishnan, "Detection of Single and Collaborative Black Hole Attack in MANET", IEEE WiSPNET 2016 conference.
[21] Hamed Samavati, Behrouz Tork Ladani and Hossein Moodi, "AMLeT: Adaptive Multi Level Trust framework for MANETs", 2011 International Symposium on Computer Networks and Distributed Systems (CNDS), February 23-24, 2011.
[22] A. Yasin and M. Abu Zant, "Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique", *Wireless Communications and Mobile Computing*, vol. 2018, 2018.
[23] ZA Zardari, J He, N Zhu et al., "A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in MANETs", *Fut Internet*, vol. 3, no. 11, 2019.